UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,586	12/22/2004	Gerardus T. M. Hubert	NL02 0587 US	9569

65913 7590 12/09/2009

NXP, B.V.
NXP INTELLECTUAL PROPERTY & LICENSING
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
12/09/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

Office Action Summary	Application No.	Applicant(s)	
	10/519,586	HUBERT, GERARDUS T. M.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2008 and 22 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46 and 48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46 and 48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 December 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. Amendment A, received on 3 December 2008, has been entered into record. In this amendment, claims 1-46 and 48 have been amended, claim 47 has been canceled.

2. Claims 1-46 and 48 are presented for examination.

Response to Arguments

3. With regards to the objections to the specification, claims, and drawings, the applicant has submitted amendments, and the examiner hereby withdraws the objections.

4. Applicant's arguments with respect to the rejection of claims 1 and 24 under 35 USC 112, second paragraph, have been fully considered and are persuasive. The rejection of 29 August 2008 has been withdrawn.

5. Applicant's arguments with respect to claims 1-46 and 48 have been considered but are moot in view of the new ground(s) of rejection.

Priority

6. The claim for priority from PCT/IB03/02623 filed on 12 June 2003 is duly noted.

Drawings

7. The drawings were received on 3 December 2008. These drawings are acceptable.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-4, 6-10, 13-17, 20, 22-27, 29-33, 36-40, 43-46, and 48 rejected under 35 U.S.C. 103(a) as being unpatentable over Daemen et al. (AES Proposal: Rijndael and Daemen hereinafter) in view of Yup et al. (US 2002/0191784 A1 and Yup hereinafter).

As to claims 1 and 24, Daemen discloses a method for a Rijndael cipher and inverse cipher in block encryption/decryption, the method having:

storing Nk words of the initial key in Nk locations of a memory (page 14, line 33);

providing the initial key to a cryptographic engine for performing a first cryptographic round (page 14, lines 33-34);

repeatedly retrieving a selected first word and a selected second word of the expanded key, at least one of which is retrieved from the memory (page 14, lines 33-34),

generating from the selected first and second words successive subsequent words of the expanded key (page 14, lines 33-34);

providing the generated words of the expanded key to the cryptographic engine as round keys for performing subsequent cryptographic rounds (page 14, lines 9-11)**;**

storing successive ones of the generated words in the memory by cyclically overwriting previously generated words of the expanded key (page 15, lines 26-28; page 17, lines 10-11)**.**

Daemen fails to specifically disclose:

maintaining four successive words from the generated words in the memory as long as they are required for use in the generation of subsequent words and for use in a parallel operation of a cryptographic process, wherein the four successive words comprise a new round key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as taught by Yup.

Yup discloses a system and method for implementing the advanced encryption standard block cipher algorithm in a system with a plurality of channels, the system and method having:

maintaining four successive words from the generated words in the memory as long as they are required for use in the generation of subsequent words and for use in a parallel operation of a cryptographic process, wherein the four successive words comprise a new round key (0013, lines 6-15; 0053, lines 13-17)**.**

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by maintaining previous words for generating subsequent words. Yup recites motivation by disclosing that using words to generate other words provides for efficiently generating round keys of the AES cipher on-the-fly in order to save RAM (0014, lines 9-12; 0015, lines 2-8). It is obvious that the teachings of Yup would have improved the teachings of Daemen by maintaining words for generating subsequent words in order to save RAM while providing for efficient on-the-fly key generation.

As to claims 2 and 25, Daemen discloses:

> **in which the step of overwriting previously generated words only occurs after said previously generated words have been used as said first and/or said second selected words while generating said subsequent words** (page 19, lines 1-2).

As to claims 3 and 26, Daemen discloses:

> **in which a number of memory locations used is less than a number of words in the expanded key** (page 14, line 33).

As to claims 4 and 27, Daemen discloses:

> **in which a number of memory locations used is equal to Nk** (page 14, line 33).

As to claims 6 and 29, Daemen discloses:

in which a number of memory locations used is equal to 2Nk (page 14, line 33; page 15, lines 26-28)**.**

As to claims 7 and 30, Daemen discloses:

in which the memory is divided into two parts, a first part storing the initial key and a second part receiving the successive words of the expanded key (page 14, lines 20-26)**.**

As to claims 8 and 31, Daemen fails to specifically disclose:

the step of completing generation of the expanded key such that a final round key is stored in the second part of the memory and the initial key is still stored in the first part of the memory.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as taught by Yup.

Yup discloses:

the step of completing generation of the expanded key such that a final round key is stored in the second part of the memory (0019, lines 5-9) **and the initial key is still stored in the first part of the memory** (0028, lines 3-5)**.**

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by storing an initial key and a final key. Yup recites motivation by disclosing that an encryption/decryption means can

selectively encrypt or decrypt data based on a control signal (0017, lines 22-26). It is obvious that the teachings of Yup would have improved the teachings of Daemen by storing an initial and final key so that encryption or decryption can be performed based on a signal.

As to claims 9 and 32, Daemen discloses:

the step of performing a repeat key expansion starting with the initial key stored in the first part of the memory (page 14, lines 33-34).

As to claims 10 and 33, Daemen fails to specifically disclose:

the step of performing an inverse key expansion starting with the final round key stored in the second part of the memory.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as taught by Yup.

Yup discloses:

the step of performing an inverse key expansion starting with the final round key stored in the second part of the memory (0019, lines 5-9).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by performing key expansion with the final key. Yup recites motivation by disclosing that storing a final key and using it for decryption does not require for the entire key expansion to be performed to get the last

key, saving processing and set-up time for decryption operations (0042, lines 6-9). It is obvious that the teachings of Yup would have improved the teachings of Daemen by starting with a stored final key for inverse key expansion in order to save processing and set-up time for decryption.

As to claims 13 and 36, Daemen discloses:

> **in which a number of memory locations used is equal to 2Nk, the first and the second parts having Nk locations each** (page 14, line 33; page 15, lines 26-28).

As to claims 16 and 39, Daemen fails to specifically disclose:

> **in which the successive subsequent words of the expanded key comprise words of encryption round keys.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as taught by Yup.

Yup discloses:

> **in which the successive subsequent words of the expanded key comprise words of encryption round keys** (0017, lines 12-20).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by using the expanded key as

encryption round keys. Please refer to the motivation recited above in respect to claims 8 and 31 as to why it obvious to apply the teachings of Yup to the teachings of Daemen.

As to claims 17 and 40, Daemen fails to specifically disclose:

> **in which the successive subsequent words of the expanded key comprise words of decryption round keys.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as taught by Yup.

Yup discloses:

> **in which the successive subsequent words of the expanded key comprise words of decryption round keys** (0019, lines 7-9)**.**

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by using the expanded key as decryption round keys. Please refer to the motivation recited above in respect to claims 8 and 31 as to why it obvious to apply the teachings of Yup to the teachings of Daemen.

As to claims 20 and 43, Daemen discloses:

> **in which the selected first word is retrieved from memory** (i.e. W[i-N_k], key) **and the selected second word is retrieved from a register used in a previous iteration** (i.e. W[i-1]) (page 14, lines 23-26)**.**

As to claims 22 and 44, Daemen discloses:

in which generating includes, in at least some cycles of round key word generation, performing an S-box transform using an S-box shared with the cryptographic engine (page 17, lines 17-18; page 18, line 18).

As to claims 23 and 45, Daemen discloses:

maintaining synchronism (i.e. parallel) **of the generation of successive round key words with consumption of the round key words by the cryptographic engine** (page 18, lines 21-25; page 19, lines 4-5).

As to claims 14 and 37, Daemen discloses:

generating successive words of AES Rijndael block cipher round keys according to an AES key expansion function (page 8, lines 30-31).

As to claims 15 and 38, Daemen fails to specifically disclose:

in which Nk=8.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as taught by Yup.

Yup discloses:

in which Nk=8 (0036, lines 1-2).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by using a key size of 8. Yup recites motivation by disclosing that having a key size of 8 requires modification to the key generation algorithm (0037, lines 1-2) because of the key size. It is obvious that the

teachings of Yup would have improved the teachings of Daemen by using a key size of 8 in order to accommodate larger key sizes by modifying the key generation algorithm.

As to claim 46, Daemen discloses:

a smart card (page 16, lines 25-26).

As to claim 48, Daemen fails to specifically disclose:

in which the initial key is maintained in the memory while generating successive subsequent words of the expanded key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as taught by Yup.

Yup discloses:

in which the initial key is maintained in the memory while generating successive subsequent words of the expanded key (0028, lines 3-5).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by keeping an initial key. Please refer to the motivation recited above in respect to claims 8 and 31 as to why it obvious to apply the teachings of Yup to the teachings of Daemen.

10. Claims 5, 11, 12, 18, 19, 21, 28, 34, 35, 41, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daemen in view of Yup as applied to claims 1 and 24 above, and further in view of Snell (US 2003/0223580 A1).

As to claims 5 and 28, Daemen in view of Yup fails to specifically disclose:

in which words of the initial key are also overwritten by words of the expanded key during the overwriting.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen in view of Yup, as taught by Snell. Snell discloses a system and method for advanced encryption standard hardware cryptographic engine, the system and method having:

in which words of the initial key are also overwritten by words of the expanded key during the overwriting (0082, lines 3-7).

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen in view of Yup with the teachings of Snell by overwriting the initial key. Snell recites motivation by disclosing that the cipher keys are needed for key expansion (0008, lines 1-2) and that decryption can be done by inverting the cipher transformations and performing the key schedule in reverse order (0009, lines 1-5). Therefore, data can be encrypted or decrypted starting with the cipher key in a certain location in order to reduce memory requirements (0011, lines 2-7). It is obvious that the teachings of Snell would have improved the teachings of Daemen in view of Yup by

overwriting an initial key in order to reduce memory requirements by storing keys needed for encryption and decryption in a single location.

As to claims 11 and 34, Daemen in view of Yup fails to specifically disclose:

> **the step of completing generation of the expanded key such that a final round key is stored in the memory and the initial key has been overwritten.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen in view of Yup, as taught by Snell. Snell discloses:

> **the step of completing generation of the expanded key such that a final round key is stored in the memory and the initial key has been overwritten** (0082, lines 3-7)**.**

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen in view of Yup with the teachings of Snell by overwriting the initial key with the final key. Please refer to the motivation disclosed above in respect to claims 5 and 28 as to why it is obvious to apply the teachings of Snell to the teachings of Daemen in view of Yup.

As to claims 12 and 35, Daemen discloses:

the step of performing an inverse key expansion starting with the final round key stored in the memory in order to regenerate the initial key for a subsequent cryptographic operation (page 22, lines 9-10).

As to claims 18 and 41, Daemen in view of Yup fails to specifically disclose:

providing the generated words on a word-by-word basis as the cryptographic engine consumes the generated words as round keys.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen in view of Yup, as taught by Snell. Snell discloses:

in which the step of providing the generated words of the expanded key to the cryptographic engine comprises providing the words on a word-by-word basis as the cryptographic engine consumes the words as round keys (0082, lines 2-10).

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen in view of Yup with the teachings of Snell by providing words word-by-word to a cryptographic engine. Snell recites motivation by disclosing that the transformation sequence in the reverse direction must be the same as that applied in the forward key expansion (0081, lines 17-19). It is obvious that the teachings of Snell would have improved the teachings of Daemen in view of Yup by providing words word-by-word in order to ensure that the proper order is executed.

As to claims 19 and 42, Daemen in view of Yup fails to specifically disclose:

in which both the selected first word and the selected second word are retrieved from the memory.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen in view of Yup, as taught by Snell. Snell discloses:

in which both the selected first word and the selected second word are retrieved from the memory (0010, lines 2-4).

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen in view of Yup with the teachings of Snell by retrieving words from memory. Snell recites motivation by disclosing that storing data in memory allows for faster subsequent execution of cryptographic rounds (0010, lines 6-7). It is obvious that the teachings of Snell would have improved the teachings of Daemen in view of Yup by retrieving data from memory in order to provide for faster execution.

As to claim 21, Daemen in view of Yup fails to specifically disclose:

in which providing the generated words of the expanded key to the cryptographic engine comprises providing said generated words from the memory.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen in view of Yup, as taught by Snell. Snell discloses:

> **in which providing the generated words of the expanded key to the cryptographic engine comprises providing said generated words from the memory** (0010, lines 2-4).

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen in view of Yup with the teachings of Snell by providing words from memory. Please refer to the motivation recited above in respect to claims 19 and 42 as to why it is obvious to apply the teachings of Snell to the teachings of Daemen in view of Yup.

Prior Art Made of Record

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Feldman et al. (US 2004/0047466 A1) discloses a system and method for advanced encryption standard hardware acceleration.

b. Okada et al. (US 2003/0108195 A1) discloses a system and method for high-speed processing in implementing the AES block cipher.

c. Ozturk et al. (US 2008/0304659 A1) discloses a system and method for expansion key generation for block ciphers.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431